



## **Acceptable Use of Information Technology Policy**

Document Name: Acceptable Use of Information Technology	Effective Date: October 15 <sup>th</sup> , 2018
Document ID: IS.002	Last Revised Date: October 4 <sup>th</sup> , 2018

### Table of contents

1. Purpose .....	2
2. Authority .....	2
3. Scope .....	2
4. Responsibility .....	2
5. Compliance .....	3
6. Policy Statements .....	3
6.1. Information Security Awareness Training .....	3
6.2. Acceptable Use of Information Assets .....	3
6.3. Information Protection .....	6
6.4. Access Management .....	7
6.5. Network Access .....	8
6.6. Physical Access .....	8
7. Related Documents .....	9
8. Document Change Control .....	9

## 1. Purpose

- 1.1. The Commonwealth of Massachusetts (“the Commonwealth”) collects, manages and stores information on a regular basis in order to support its organizational operations. The Commonwealth is committed to preserving the confidentiality, integrity, and availability of its **information assets**<sup>1</sup>.

The Commonwealth must protect its information assets, provide for the integrity of organizational processes and records, and comply with applicable laws and regulations.

This document, the *Acceptable Use of Information Technology Policy*, documents the responsibilities of all Commonwealth Executive Offices and Agencies within executive offices. Agencies and offices are required to implement procedures that ensure their **personnel**, including vendors, contractors, and consultants, comply with requirements in regard to safeguarding information owned or entrusted to the Commonwealth.

## 2. Authority

- 2.1. M.G.L. Ch. 7d provides that “Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology.”

## 3. Scope

- 3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to all state agencies in the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document, with respect to those services, as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their **personnel** comply with the requirements herein to safeguard information.

## 4. Responsibility

- 4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this **policy**.
- 4.2. The Enterprise Security Office is responsible for monitoring compliance with this policy and may enlist other departments to assist in the enforcement of this policy.
- 4.3. Any inquiries or comments regarding this policy shall be submitted to the Enterprise Security Office by contacting the Security Program Office at [EOTSS-DL-Security Office](#).
- 4.4. Additional information regarding this policy and its related standards may be found at <https://www.mass.gov/cybersecurity/policies>.

---

<sup>1</sup> Words in **bold italics** are defined in the Glossary (section 6).

## 5. Compliance

- 5.1. Compliance with this document is mandatory for all state agencies in the Executive Department. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the Security Office ([EOTSS-DL-Security Office](#)). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

## 6. Policy Statements

### 6.1. Information Security Awareness Training

The Commonwealth is committed to establishing an information security-aware culture to help protect its information assets. To support this goal, the Commonwealth has established the following practices:

- 6.1.1 New hires: All new hires must complete security awareness training within the established new hire training timeline and regularly thereafter. Records demonstrating the completion of such training shall be maintained and reported to the employee's manager. Security awareness will be made easily available for Commonwealth Agencies and Offices to provide to state employees.
- 6.1.2 Ongoing: All Commonwealth Agencies and Offices must ensure that their personnel participate in regular information security awareness training, including mandatory participation in periodic social engineering (e.g., phishing) training exercises. Records demonstrating the completion of such training shall be maintained and reported to the Enterprise Security Office.
- 6.1.3 Job-specific: Commonwealth agencies may have some job functions that require additional information security training. The agency will provide the additional training requirements as needed. Examples may include personnel who have access to systems that store confidential information or job responsibilities such as Developers and database Administrators. The Commonwealth CISO determines the job functions that require additional training.

A quarterly training report will be sent to the Enterprise Security Office to track overall completion rates.

### 6.2. Acceptable Use of Information Assets

The Commonwealth's information assets further organizational goals and priorities. In using the Commonwealth's information assets, Commonwealth Executive Offices and Agencies should encourage their personnel act in a professional and ethical manner and comply with their applicable *Code of Conduct*, relevant enterprise, and agency-level policies and/or applicable contractual obligations.

#### 6.2.1 Use of information technology resources

- 6.2.1.1 It is unacceptable for any person to use agency information technology resources:

- 6.2.1.1.1 In furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal
- 6.2.1.1.2 For any political purpose
- 6.2.1.1.3 For any commercial purpose
- 6.2.1.1.4 To send threatening or harassing messages, whether sexual or otherwise
- 6.2.1.1.5 To access or share sexually explicit, obscene or otherwise inappropriate materials
- 6.2.1.1.6 To infringe any intellectual property rights
- 6.2.1.1.7 To gain, or attempt to gain, unauthorized access to any computer or network
- 6.2.1.1.8 For any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs
- 6.2.1.1.9 To intercept communications intended for other persons
- 6.2.1.1.10 To misrepresent either the agency or a person's role at the agency
- 6.2.1.1.11 To distribute chain letters
- 6.2.1.1.12 To access online gambling sites
- 6.2.1.1.13 To libel or otherwise defame any person

#### 6.2.2 Email use

The following instructions are designed to prevent personnel from engaging in harmful email practices:

- 6.2.2.1 Do not use email accounts for commercial purposes unrelated to Commonwealth business.
- 6.2.2.2 Do not conduct government business through or send **confidential information** to a personal email account.
- 6.2.2.3 Do not send **confidential information** to any recipient not authorized to receive such information.
- 6.2.2.4 Do not use email to transmit **confidential information** in an unencrypted format.
- 6.2.2.5 Do not collect and/or transmit material in violation of any federal, state, or local law or organizational policy.

#### 6.2.3 Use of technology assets

Personnel must use the Commonwealth's technology assets appropriately and comply with the following requirements:

- 6.2.3.1 Do not download or install unauthorized (e.g., unlicensed, pirated) software onto Commonwealth-issued devices.

- 6.2.3.2 Avoid excessive use of system information technology resources for personal use, including but not limited to network capacity (e.g., high use of video streaming technologies).
- 6.2.3.3 Do not circumvent, attempt to circumvent, or assist another individual in circumventing the information security controls in place to protect Commonwealth-issued devices.

#### 6.2.4 Secure transfer of information

- 6.2.4.1 **Confidential information** shall be securely exchanged through only authorized methods. **Confidential Information** shall not be electronically transferred in an unencrypted or unprotected format. Refer to Cryptography Policy for additional details on data protection.

#### 6.2.5 Record retention

- 6.2.5.1 Information storage and retention time frames shall be limited to what is required for legal, regulatory and business purposes.

#### 6.2.6 Secure workspace

- 6.2.6.1 Personnel must keep their assigned workspace secure (e.g., lock confidential information in drawers, use cable locks if issued by Commonwealth).
- 6.2.6.2 Personnel must be mindful of using mobile devices (e.g., smartphones and tablets) with access to Commonwealth information. Mobile devices must be secured with a password that meets or exceeds the **access control** requirements and must not be left unattended.
- 6.2.6.3 When personnel are telecommuting or working remotely, Commonwealth-owned devices must not be left unattended in public spaces, such as on public transportation, in a restaurant or coffee shop, or in a doctor's office.
- 6.2.6.4 Documents containing **confidential information** that are sent to a shared printer must be retrieved immediately to reduce the risk of unauthorized access.

#### 6.2.7 Privacy and monitoring

The use of Commonwealth-owned information systems and assets is subject to monitoring and review.

- 6.2.7.1 Personnel should have no expectation of privacy with respect to the Commonwealth's communications systems.
- 6.2.7.2 Commonwealth's communications systems (e.g., emails, instant messages, Internet usage) may be monitored, logged, reviewed, recorded and/or investigated.
- 6.2.7.3 Records of activity on these systems may be used by the Commonwealth and/or turned over to law enforcement authorities and other third parties.
- 6.2.7.4 Personnel must be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic.
- 6.2.7.5 The agency retains, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the agency

will exercise the right to inspect any user's computer, any information contained in it, and any information sent or received by that computer.

### 6.3. Information Protection

6.3.1 Information classification. All Commonwealth Executive Offices and Agencies must ensure that state employees/personnel adhere to these requirements.

6.3.1.1 Personnel must adhere to the information classification system and ensure that appropriate measures are taken to protect information commensurate with its value to the Commonwealth. The information classification system includes Confidential, Internal Use and Public. See section 6, Glossary for definitions and see Information Classification in the Asset Management Standard for additional details.

### 6.3.2 Information protection requirements

The confidentiality and integrity of information must be protected at rest, in use and in transit. Personnel must adhere to the following guidelines.

Information governed by compliance standards requires additional information protection requirements that are not addressed in this policy.

#### 6.3.2.1 Information at rest

The following are guidelines to safeguard confidential information at rest:

- 6.3.2.1.1. Store all information on access-restricted and/or -controlled Shared Folders or Drives (e.g., SharePoint).
- 6.3.2.1.2. Encrypt or password-protect removable media that contains confidential information such as USB drives and mobile devices.
- 6.3.2.1.3. Dispose of confidential information only after confirming compliance with records retention laws.

#### 6.3.2.2 Information in use

The following are guidelines to safeguard confidential information in use:

- 6.3.2.1.4. For access to systems that host confidential information, personnel must request access using an approved access request process/tool and be positively authenticated (i.e., have an established user identity in Active Directory or another authentication source).
- 6.3.2.1.5. Use the minimum amount of **confidential information** (such as Social Security numbers) to the minimum necessary to support business operations (e.g., last four digits). Store the information in approved information repositories.
- 6.3.2.1.6. Where possible, do not store confidential information on laptops or desktops. Confidential information must be stored in Shared Folders, Shared Drives, or other secure Commonwealth systems.

#### 6.3.3.2. Information in transit

Use Commonwealth-issued encryption solutions to protect the integrity of confidential information that will be transmitted outside of the Commonwealth. This can be achieved by the following:

- 6.3.3.3.1 Use secure mail feature of email client by adding “[secure]” in the subject line to encrypt the email.
- 6.3.3.3.2 Password-protect files that contain confidential information (See IS.008 Cryptographic Management Standard).
- 6.3.3.3.3 Use the Commonwealth-approved secure transfer solution for larger transfers.

#### 6.4. Access Management

Agencies and offices must ensure that personnel are positively authenticated and authorized prior to receiving access to Commonwealth information resources. Access to systems shall be based on the user’s role and must be limited to the minimum rights necessary to perform his or her job function. Access to information assets must be controlled through a defined process, which includes a periodic review of information system privileges. (Refer to Access Management Policy)

##### 6.4.1 User access to information systems

- 6.4.1.1 Authorization: Users must have an active user ID to access information assets on the Commonwealth family of networks.
- 6.4.1.2 Authentication: Information assets that access or store confidential information must authenticate a user’s identity (e.g., password) prior to granting access.
- 6.4.1.3 Access requests: Users must request access to technology infrastructure and/or applications required for job responsibilities using the Commonwealth-approved access request tools.
- 6.4.1.4 Least privilege: Users must not be granted access to technology infrastructure and/or applications that are not required to perform his/her job responsibilities. Managers are responsible for ensuring their direct reports have the appropriate access to systems.
- 6.4.1.5 Reviews of user’s access to applications and/or technology infrastructure will be performed by Managers at least annually to ensure access is appropriate to perform his/her job responsibilities.
- 6.4.1.6 Segregation of duties: Users must not be granted access to information assets that would allow entitlements to perform job responsibilities that are not compatible with each other (e.g., having the ability to both request and approve a change).

##### 6.4.2 Protect your password

Passwords provide a foundational security control to protect access to systems, technology infrastructure, applications and information.

- 6.4.2.1 Do not reveal passwords to others or allow others to use your passwords.
- 6.4.2.2 Maintain passwords in a secure manner. Do not write down or store passwords in an insecure manner.

6.4.2.3 Change default passwords upon the first login.

6.4.2.4 Passwords must be designed to meet the risks and threats of the technology environment and comply with the password standard, as follows:

6.4.2.4.1 Passwords shall be a minimum of twelve (12) characters and include all four (4) of the following characteristics:

- Special characters (e.g., ' , % , \$ , #)
- Alphabetic characters (e.g., a , b , c)
- Combination of uppercase and lowercase letters
- Numerical characters (e.g., 1 , 2 , 3)

6.4.2.4.2 New passwords must be different from the previous nine passwords.

6.4.2.4.3 The password standard is enforced by systemic controls. Administrative access may require longer and more complex passwords. See *Access Management Standard* for additional details.

## 6.5. Network Access

Commonwealth network access is restricted to authorized users only. Users must have a domain user identity to access the network.

### 6.5.1 Wireless Access

To improve mobility, connectivity and collaboration opportunities, the Commonwealth provides two wireless (wifi) networks, 'secured' and 'public', at certain office locations. Users must be aware that not all internal applications will be available through the public wifi. Personnel who wish to use wireless connections to conduct Commonwealth business may be required to connect to the secured wifi.

### 6.5.2 Remote Access

Users who access the Commonwealth network remotely must be authenticated prior to establishing a network connection.

## 6.6. Physical Access

Commonwealth facilities and information assets must have appropriate physical access controls to protect them from unauthorized access. The important points that must be considered in physical security are as follows:

6.6.1 Users must have a Commonwealth-issued badge and be prepared to show it if requested by building security.

6.6.2 Only authorized persons are allowed into access-controlled areas. Visitors are allowed but must be escorted in controlled areas.

6.6.3 Circumventing established access control systems (e.g., propping doors open or tampering with turnstiles) is prohibited.



## 2. Related Documents

Document	Effective date
Code of Conduct (business unit specific)	
Cryptographic Management Policy	
Asset Management Standard	
Access Management Standard	

## 3. Document Change Control

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/02/2018	Corrections and formatting.
0.95	Sean Vinck	5/7/2018	Corrections and formatting.
0.96	Andrew Rudder	5/31/18	Corrections and formatting.
0.97	Anthony O'Neill	05/31/2018	Corrections and formatting.
1.0	Dennis McDermitt	6/1/2018	Final Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement must be submitted to the document owner.

### 6.6. Annual Review

This *Acceptable Use of Information Technology Policy* must be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.